

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-207695

(43)Date of publication of application : 07.08.1998

(51)Int.Cl. G06F 7/58
G09C 1/00
H03K 3/84

(21)Application number : 09-005335

(71)Applicant : NEC IC MICROCOMPUT SYST LTD

(22)Date of filing : 16.01.1997

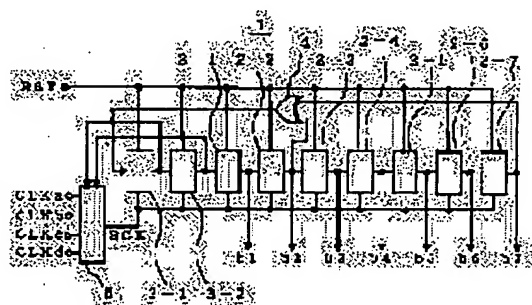
(72)Inventor : TANAKA MASANORI
ISHIMOTO JUNICHI

(54) PSEUDORANDOM NUMBER GENERATION CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To make it difficult to analyze circuit constitution from a generated random number string.

SOLUTION: A linear feedback shift register 1 is constituted of registers 2-1 to 2-7 corresponding to the bit width of a generated random number, redundant registers 3-1, 3-2 and an exclusive OR circuit 4. A decoder/multiplexer 5 selects one of internal clocks CLKa to CLKd in accordance with the output values of the registers 3-1, 3-2 and outputs the selected clock as a shift clock SCK for the register 1. Consequently the period of the shift clock SCK for the register 1 can be provided with irregularity.



LEGAL STATUS

[Date of request for examination] 16.01.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2937919

[Date of registration] 11.06.1999

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office